

Threat Mitigation & Collective Defense

Protecting our Critical Infrastructure

DOE's Cyber Fed Model (CFM)

Scott Pinkerton

pinkerton@anl.gov

www.anl.gov/it/cfm

Agenda

- Collective Defense
- Protecting Infrastructure
- Relationships are Key
- DOE's CFM
- 2011 Roadmap
- Subscription vs. Participation
- What's in it for me ?
- Conclusions & Take Aways
- Questions



Collective Defense

- Microsoft's Scott Charney (VP Trustworthy Computing) gave a keynote at RSA 2011 titled "Collective Defense: Collaborating to create a safer Internet"
- Makes sense if you believe in a common adversary
- Argonne started working on collective defense in 2004
 - Two different computer break-ins followed by a scathing Washington Post article
 - Initial efforts with NCSA

Protecting our IT Infrastructure

- At the local (single site) level, security goals are simple
 - Keep the “bad guys” out
 - Let the “good guys” in
 - Keep wheels turning – business
 - Protect our interests - \$\$, data
- Protecting Infrastructure – hard
 - Increasing skill & sophistication of the bad guys
 - Standardized technology & common vulnerabilities
 - Increasing degree of connectivity & inter-dependence
 - Increasing risk with criticality of systems & data on-line today



Skill & Sophistication of the Bad Guys

A global cybercrime syndicate broke into an encrypted file containing ATM passwords. Within 12 hours the group had accessed 2,100 ATM machines in 280 cities on three continents and made over 14,000 ATM transactions. In one day, the group stole more than \$9 million.

Source: FOSE Keynote Speech, March 23, 2010

Steven R. Chabinsky, Deputy Assistant Director, Cyber Division of the FBI

Patching the typical end-user PC

Source: Secunia, Stefan Frei

- Of the top 50 PC applications (26 from Microsoft and 24 3rd party applications) – there are 14 different vendors
- One update mechanism covers the OS and 26 Microsoft programs (35% of the CVE vulnerabilities)
- Another 13 different update mechanisms required to patch the remaining 24 applications, and more importantly 65% of the CVE vulnerabilities

Establishing Trusted Collaborations

- This part is hard
 - Really hard
- Technology issues aren't too complex
 - Compared to MOU/ ISA / NDA (legal) issues
- Relationships are the key



DOE Cyber Fed Model (CFM)

- Theory is simple
 - Detect threats locally
 - Protect & Defend Globally
- **Practice is a bit harder**



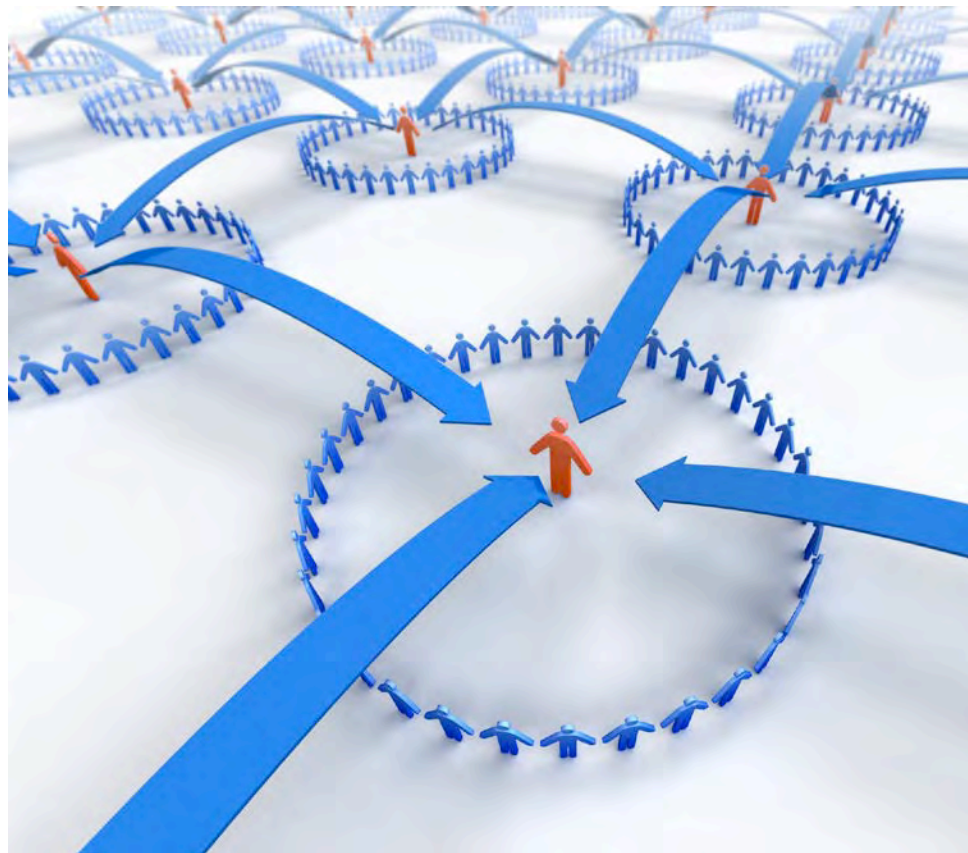
In Practice ...

- Every organization is a snowflake
 - B2B / collaborations vary
 - Blocking anything can be highly disruptive
- Know your network – 1999
 - Know your data – 2005
 - Know your **relationships** – 2010

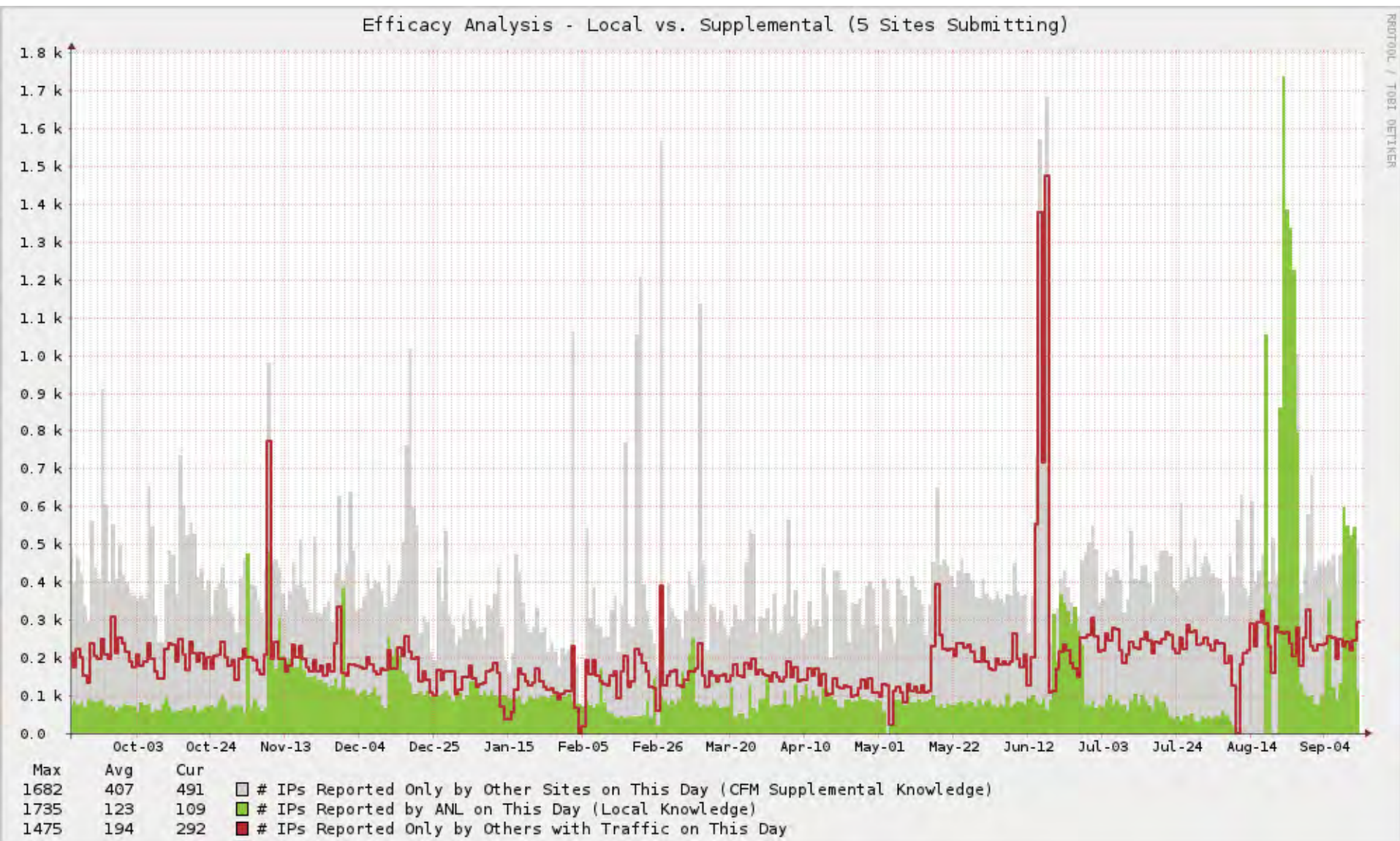


Cyber Fed Model (CFM) is ...

- A near real-time exchange of actionable alerts
 - Information on IP addresses, DNS names, URL's, e-mail
- Focused on autonomic machine-machine communication to actively modify perimeter protection (blocking)
- Strongly promoting the sharing of best in breed detection tools (IDS signatures, algorithms, etc.)



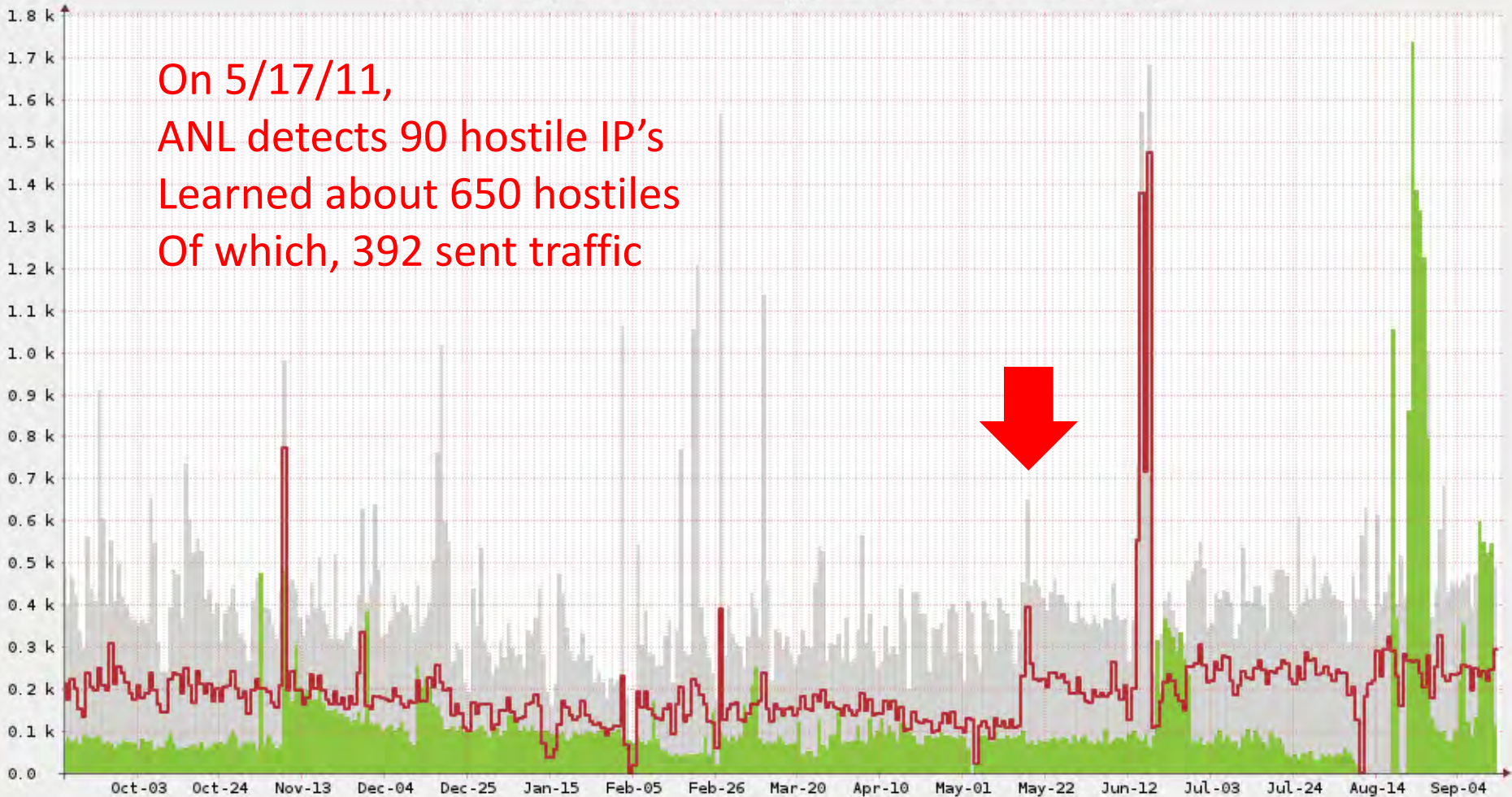
Local vs. *Federated* Knowledge



Relevance & ROI

Efficacy Analysis - Local vs. Supplemental (5 Sites Submitting)

On 5/17/11,
ANL detects 90 hostile IP's
Learned about 650 hostiles
Of which, 392 sent traffic



Max	Avg	Cur	
1682	407	491	□ # IPs Reported Only by Other Sites on This Day (CFM Supplemental Knowledge)
1735	123	109	■ # IPs Reported by ANL on This Day (Local Knowledge)
1475	194	292	■ # IPs Reported Only by Others with Traffic on This Day

Roadmap to Achieve Energy Delivery Systems Cyber Security

- Strategy #5 – Sustain Security Improvements
 - 5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders
 - 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector

Sharing actionable cyber threat information can be done today !

Subscription vs. Active Participation

- Can you just subscribe to a “feed” of hostile IP addresses and just download them ?
 - Sure, there are a growing number of “reputational” subscription services
 - But will they be **RELEVANT** to you – assuming none of the energy owner/operators are contributors

IP's exploiting
MS problem
dujour

IP's exploiting
Adobe problem
dujour

IP's sending
spam e-mail
farming for
username/PW

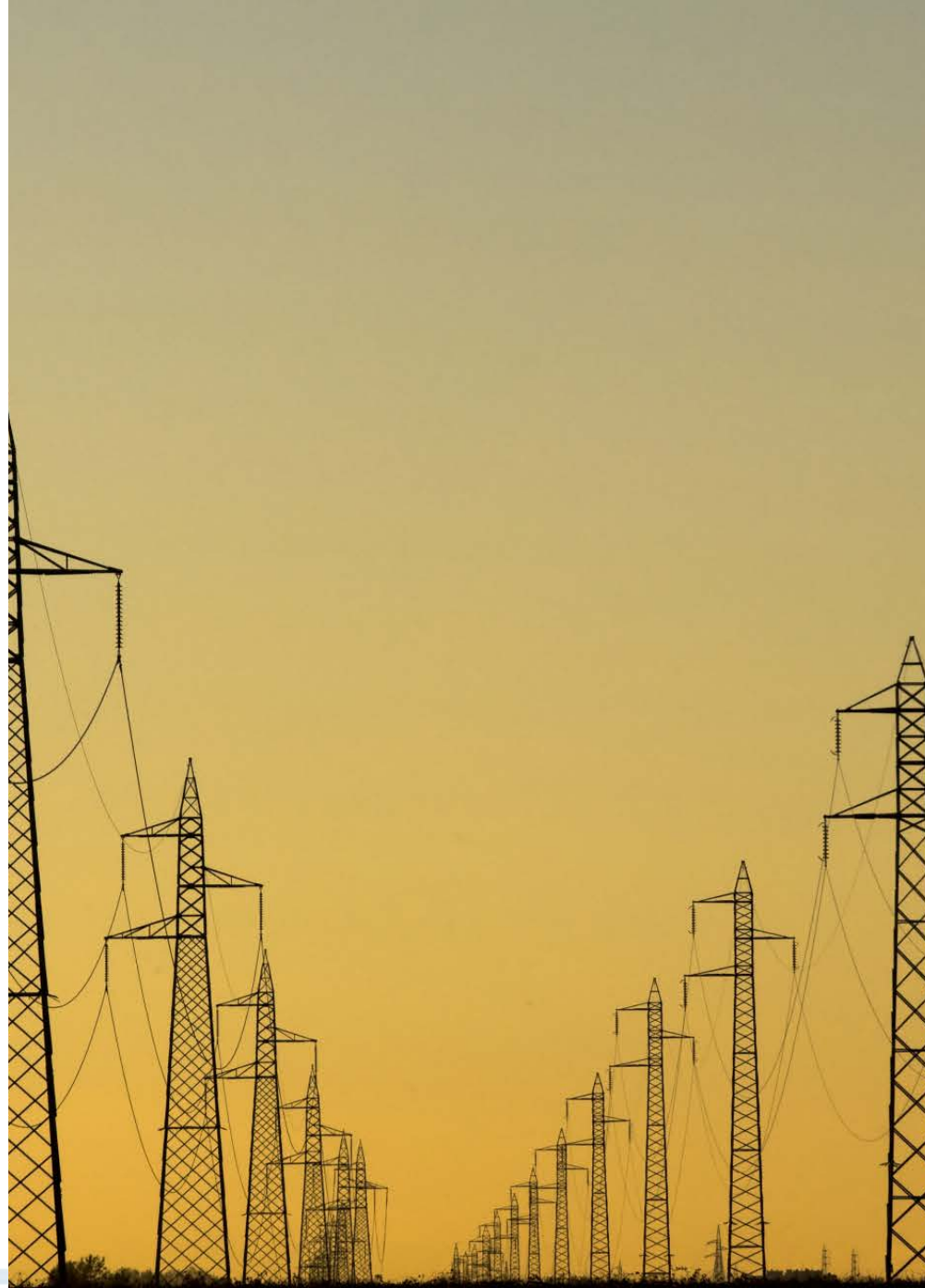
IP's sending
spam e-mail
farming for
bank account

IP's probing
for ssh
servers

IP's looking to
attack the
Energy Infra.

What can Collective Defense do for me ?

- Actively sharing actionable cyber threat information can significantly increase effectiveness of local IDS
 - With very little cost
- Encourage active participation and NOT just subscription



Conclusions & Take Aways

- Disappearing boundaries – at risk from people who no longer require physical proximity
- Speed and volume of Internet threats dictate we improve our response time to act and re-act
- Technology alone will not save us



Questions ??

Scott Pinkerton

pinkerton@anl.gov

www.anl.gov/it/cfm